

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

---

CRUM & FORSTER SPECIALTY  
INSURANCE COMPANY,

Plaintiff

Case No. \_\_\_\_\_

v.

COMPLAINT IN INTERPLEADER OF  
CRUM & FORSTER SPECIALTY  
INSURANCE COMPANY

FINANCIAL BUSINESS AND CONSUMER  
SOLUTIONS, INC., CHRISTINE C.  
SHUBERT, as Chapter 7 Trustee of  
FINANCIAL BUSINESS AND CONSUMER  
SOLUTIONS, INC., TRANSWORLD  
SYSTEMS, INC., CASCADE RECEIVABLES  
MANAGEMENT LLC, HARVEST  
STRATEGY GROUP, KOHL'S, INC.,  
CAVALRY PORTFOLIO SERVICES, LLC,  
and INVESTINET, LLC,

Defendants.

---

Plaintiff Crum & Forster Specialty Insurance Company ("C&F"), by its undersigned counsel, hereby files this action in interpleader against Defendants, and for its claim for relief alleges as follows.

**NATURE OF THE ACTION**

1. This is an action in interpleader brought pursuant to 28 U.S.C. §§ 1335, 1397, and 2361, to resolve the competing claims of the Defendants for amounts Defendants seek or may seek from the insurance policy issued by C&F to Defendant Financial Business and Consumer Solutions, Inc. ("FBCS").

2. As described more fully below, C&F issued Excess Liability Policy No. CYB-107007 (the "Excess Policy") to FBCS, which applies in excess of and follows form to Corvus

Smart Cyber Insurance Policy No. CYB-107946258-00, which Travelers Excess and Surplus Lines Company (“Travelers”) issued to FBCS (the “Primary Policy,” together with the Excess Policy, the “Policies”). The Excess Policy provides, among other types of coverage, and subject to its and the Primary Policy’s terms, conditions, exclusions, and limitations, certain first-party and third-party liability coverage to FBCS and others who constitute **Insureds**<sup>1</sup> under the Policies.

3. FBCS and the Putative Additional Insureds (defined and discussed below) have sought coverage under the Excess Policy in connection with the underlying Cyber Incident (defined and discussed further below). C&F also expects to receive additional demands for payments under the Excess Policy in connection with the Cyber Incident.

4. C&F reasonably believes that demands for payment from the Excess Policy will exceed the maximum aggregate limit of liability of the Excess Policy. In the face of conflicting and competing demands for payment of **Defense Expenses, Breach Response and Remediation Expenses, and Breach Management Expenses**, potential future judgments against one or more of the **Insureds**, and/or potential settlements, C&F brings this action in interpleader for the Court to determine how to allocate the Excess Policy proceeds among these competing demands.

### **JURISDICTION AND VENUE**

5. This Court has jurisdiction of the case under 28 U.S.C. § 1335 because: (a) it is a civil action in interpleader filed by a corporation that issued an insurance policy with limits of \$500 or more; (b) there are two or more adverse claimants of diverse citizenship who demand or may demand the right to payment of money of the value of \$500 or more, which is in the custody or possession of C&F; and (c) concurrently with the filing of this Complaint, or as soon thereafter as possible, C&F will deposit the aggregate limits of the Excess Policy into the registry of the

---

<sup>1</sup> Except for headings herein, terms in **bold** are defined in the Policies.

Court, to abide the future order or judgment of the Court with respect to the subject matter of the controversy.

6. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b). Venue is proper in this federal district pursuant to 28 U.S.C. § 1397 because one or more of the claimants reside in this judicial district.

### **THE PARTIES**

7. Plaintiff Crum & Forster Specialty Insurance Company is an insurance company that is organized and existing under the laws of the State of Delaware, with its principal place of business in New Jersey.

8. Upon information and belief, Defendant Financial Business and Consumer Solutions, Inc. (“FBCS”) is a company that is organized and existing under the laws of the State of Pennsylvania, with its principal place of business at 330 S. Warminster Road, Suite 353, Hatboro, Pennsylvania 19040.

9. Defendant Christine C. Shubert (“Trustee”) is the duly appointed trustee of the Chapter 7 estate of FBCS in *In re: Financial Business and Consumer Solutions, Inc.*, Case No. 24-13029-AMC (U.S. Bankruptcy Court for the Eastern District of Pennsylvania) (the “Bankruptcy Case”). Ms. Shubert has a usual place of business at 821 Wesley Avenue, Ocean City, New Jersey 08226.

10. Upon information and belief, Defendant Transworld Systems, Inc. (“TSI”) is a company that is organized and existing under the laws of the State of Delaware, with its principal place of business in Delaware.

11. Upon information and belief, Defendant Cascade Receivables Management LLC (“Cascade”) is a company that is organized and existing under the laws of the State of Delaware, with its principal place of business in California.

12. Upon information and belief, Defendant Harvest Strategy Group (“Harvest”) is a company that is organized and existing under the laws of the State of Colorado, with its principal place of business in Colorado.

13. Upon information and belief, Kohl’s, Inc. (“Kohl’s”) is a company that is organized and existing under the laws of the State of Delaware, with its principal place of business in Wisconsin.

14. Upon information and belief, Defendant Cavalry Portfolio Services, LLC (“Cavalry”) is a company that is organized and existing under the laws of the State of Delaware, with its principal place of business in New York.

15. Upon information and belief, Defendant InvestiNet, LLC (“InvestiNet”) is a company that is organized and existing under the laws of the State of South Carolina, with its principal place of business in South Carolina.

16. All of the foregoing defendants are hereinafter referred to collectively as the “Defendants,” and Defendants TSI, Cascade, Harvest, Kohl’s, Cavalry, and InvestiNet are hereinafter collectively referred to as the “Putative Additional Insureds.”

17. All of the Defendants have made, or may potentially make, demands for proceeds of the Excess Policy.

## **FACTS**

### **The Policies**

#### **The Primary Policy**

18. Travelers issued the Primary Policy to FBCS for the February 1, 2024 to February 1, 2025 Policy Period. Exhibit A to this Complaint is a true and correct copy of the Primary Policy, which is incorporated as if fully stated herein.

19. The Primary Policy, subject to its terms, conditions, and exclusions, has limits of liability of \$5 million Each **Claim** or **Loss**, subject to a \$5 million Aggregate Limit of Liability, in excess of a \$50,000 Each **Claim/Loss** Retention. *See* Ex. A, Declarations, Item 5 (pp. 4-5 of 71).

20. Subject to all of its terms, conditions, and exclusions, the Primary Policy affords certain first-party and third-party liability insurance coverage to “**Insureds**,” which means, among other things, FBCS and “[a]ny legal entity required by written contract to be named as an additional insured under this Policy.” *Id.*, Definitions, as amended by CRC Smart Cyber Amendatory Endorsement (p. 46 of 71).

21. Subject to all of its terms, conditions, and exclusions, the Primary Policy provides certain types of first-party and third-party liability insurance coverage arising out of a “**Security Breach**” or “**Privacy Breach**.” *See id.*, Third Party Insuring Agreements and First Party Insuring Agreements (pp. 10-11 of 71).

22. “**Security Breach**” includes, among other things, “The use of the **Computer System** by an unauthorized person or persons, or by an unauthorized person in an unauthorized manner, including social engineering techniques[.]” *Id.*, Definitions (p. 25 of 71).

23. “**Computer System**” means “A system of interconnected hardware and peripherals, and associated software, including Internet of Things (IoT) devices, systems and

application software, terminal devices, related communication networks, mobile devices, storage and back-up devices, and industrial systems operated by the **Insured** or an **Outsourced Service Provider**.” *Id.*, Definitions, as amended by CRC Smart Cyber Amendatory Endorsement (p. 44 of 71).

24. “**Privacy Breach**” means “a. A breach of confidentiality, or infringement or violation of any right to privacy, or a breach of the **Named Insured’s** privacy policy or of **Privacy Regulations**; or b. An accidental release, unauthorized disclosure, loss, theft or misappropriation of **Protected Personal Information** or confidential corporate information in the care, custody or control of an **Insured** Entity or **Outsourced Service Provider**; [or] c. A failure to prevent a privacy breach or failure to implement, maintain, or comply with privacy policies and procedures that identify the Insured's obligations relating to Protected Personal Information, including but not limited to the Insured's privacy policy.” *Id.*

25. “**Protected Personal Information**” means:

With respect to natural persons, any private, non-public information of any kind in an **Insured’s** care, custody, or control, regardless of the nature or form of such information, including but not limited to the following, but only if such information allows an individual to be uniquely identified:

- a. Social security number;
- b. Medical service or healthcare data;
- c. Driver’s license or state identification number;
- d. Equivalents of any of the information listed in a.-c. above;
- e. Account, credit card, or debit card number, alone or in combination with any information that permits access to an individual’s financial information, including, but not limit to, security or access code or password; and
- f. Other-non-public information to the extent prescribed under **Privacy Regulations**;

However, **Protected Personal Information** does not mean publicly available information that is lawfully in the public domain or information available to the general public from government records[.]

*Id.*, Definitions (p. 24 of 71).

26. Among other things, and subject to all of its terms, conditions, and exclusions, the Primary Policy provides coverage for “**Damages and Defense Expenses** which the **Insured** is legally obligated to pay as a result of a **Claim** arising from a **Security Breach or Privacy Breach.**” *Id.*, Third Party Insuring Agreements, Section I.A., Network Security and Privacy Liability (p. 10 of 71).

27. “**Claim**” is defined to include, among other things, “notice of an intention to hold the **Insured** responsible for **Damages**, including the service of legal proceedings, the institution of arbitration or mediation, or a written request to toll or waive a statute of limitations against any of the **Insureds**[.]” *Id.*, Definitions, as amended by CRC Smart Cyber Amendatory Endorsement (p. 42 of 71).

28. Among other things, and subject to all of its terms, conditions, and exclusions, the Primary Policy provides coverage for “**Breach Management and Incident Response Expenses** which the **Insured** has contractually indemnified a **Third Party** for a **Security Breach or Privacy Breach** when the **Insured** has a legal obligation to notify affected individuals.” *Id.*, Third Party Insuring Agreements, Section I.E., Breach Management Expenses (p. 10 of 71).

29. Among other things, and subject to all of its terms, conditions, and exclusions, the Primary Policy provides coverage for “**Breach Management and Incident Response Expenses** incurred directly as a result of a **Privacy Breach or Security Breach.**” *Id.*, First Party Insuring Agreements, Section II.H., Breach Response and Remediation Expenses (p. 11 of 71).

30. “**Breach Management and Incident Response Expenses**” is defined in full to mean:

- a. Costs of an external IT security expert to determine the cause, scope and extent of the **Privacy Breach or Security Breach** or any immediate actions necessary to mitigate ongoing harm to the **Insured’s Computer System**;

- b. Costs and expenses of a legal firm to determine any actions necessary to comply with **Privacy Regulations**;
- c. Notification costs and related expenses to notify:
  - I. Individuals who are required to be notified in compliance with **Privacy Regulations** mandating notifications; or
  - II. Any individual affected by the actual or suspected cyber event or to send email notices or issue substitute notices;
  - III. Costs of setting up a telephone call center in order to support notified individuals and to provide credit file monitoring services and/or identity theft assistance;
- d. **Crisis Management Expenses**;
- e. Costs to provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals for up to 24 months.
- f. Access to **Company's** 24/7 Cyber Incident Response Hotline;
- g. Costs to obtain initial report support and assistance from the **Company**;
- h. Costs to conduct a forensic investigation of the **Insured's Computer System** where reasonable and necessary or as required by law or a regulatory body (including a requirement for a PCI Forensic Investigator);
- i. Costs to contain and remove any malware discovered on the **Insured's Computer Systems**;
- j. Costs to complete an information security risk assessment; [or]
- k. Costs to conduct an information security gap analysis[.]

However, the **Company** will only indemnify the **Breach Management and Incident Response Expenses** in paragraphs a. through k. above if such costs and expenses are reasonable and necessary, and are incurred by the **Insured** with the **Company's** prior written consent.

**Breach Management and Incident Response Expenses** does not include any:

- 1. internal costs or expenses incurred by any **Insured**;
- 2. **Extortion Expenses**;
- 3. or **Extortion Payment**.



The **Company** has the right to select and appoint any vendors, external IT security experts, breach coach, or legal counsel providing services in connection with **Breach Management and Incident Response Expenses**.

*Id.*, Definitions, as amended by Smart Cyber Insurance Amendatory Endorsement (pp. 16-17 and 60 of 71).

The Excess Policy

31. C&F issued the Excess Policy to FBCS for the February 1, 2024 to February 1, 2025 Policy Period. Exhibit B to this Complaint is a true and correct copy of the Excess Policy, which is incorporated as if fully stated herein.

32. The Excess Policy, subject to its terms, conditions, and exclusions, has an aggregate limit of liability of \$5 million, in excess of the \$5 million aggregate limit of the Primary Policy. *See* Ex. B, Declarations, Items 3-4 and 9.

33. Subject to all of its terms, conditions, and exclusions, the Excess Policy's Insuring Agreement provides:

This Policy shall provide coverage in accordance with the same terms, conditions and limitations of the **Followed Policy**, as modified and subject to the terms, conditions and limitations of this Policy.

The **Insurer's** coverage obligations under this Policy attach to the **Insurer** only after the **Total Underlying Limits** have been exhausted through payments by, on behalf of or in the place of the **Underlying Insurers** of amounts covered under the **Underlying Policies**. This Policy shall continue in force as primary insurance only upon the exhaustion of the **Total Underlying Limits** by reason of such payments and satisfaction of any applicable retention. This Policy shall recognize erosion of an **Underlying Limit** of an **Underlying Policy** through payments by others of covered amounts under that **Underlying Policy**. The risk of uncollectibility of any part of the **Total Underlying Limits**, for any reason, is expressly retained by the **Policyholder** and any insureds, and is not insured under this Policy or assumed by the **Insurer**.

*Id.*, Section I.

34. The Excess Policy specifies that the “**Followed Policy**” and “**Underlying Policy**” refer to the Primary Policy, the “**Underlying Insurer**” is Travelers, and the “**Underlying Limit**” and “**Total Underlying Limits**” are the \$5 million aggregate limit of liability of the Primary Policy. *See id.*, Declarations, Items 4 and 9.

#### **The Cyber Incident and Costs Incurred to Date**

35. On February 27, 2024, FBCS reported to C&F that it had discovered a network incident and filed a claim with Travelers, and was also notifying C&F of the incident under the Excess Policy (the “Cyber Incident”).

36. According to a “Notice of Data Event” published on FBCS’s website (*see* [Cyber Incident - FBCS, Inc. \(fbc-inc.com\)](https://www.fbcinc.com/cyber-incident)):

On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS’s network. FBCS immediately took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. FBCS determined that the environment was subject to unauthorized access between February 14, 2024, and February 26, 2024. The unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Therefore, FBCS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. FBCS is now providing notice to potentially impacted individuals. This notification was not delayed as a result of a law enforcement investigation.

FBCS determined that the type of information that may have been impacted varies per person and may include consumer name, address, date of birth, Social Security number, driver’s license number, other state identification number, medical claims information, provider information, and clinical information (including diagnosis/conditions, medications, and other treatment information), and/or health insurance information. FBCS takes the confidentiality, privacy, and security of information in our care seriously. Upon discovering this incident, we immediately took steps to conduct a diligent investigation to confirm the nature and scope of the incident. This matter has also been reported to federal law enforcement. As part of FBCS’s ongoing commitment to the security of information on our platform, we also implemented additional safeguards in a newly built environment.

37. FBCS has incurred and will continue to incur various costs and/or requests for reimbursement in connection with the Cyber Incident, including but not limited to data mining and forensic investigation costs, notification to data owners, indemnification of FBCS's clients for their costs of notifying consumers whose data was potentially impacted, and responses to requests for information from regulatory agencies.

38. On information and belief, Travelers has paid or reimbursed some or all of the foregoing costs from the Primary Policy.

39. As of August 21, 2024, approximately \$230,000 remained of the limits of liability of the Primary Policy.

40. On information and belief, FBCS's remaining costs in connection with ongoing forensic investigation and consumer notifications, among other things, is estimated at over \$1 million.

41. Accordingly, FBCS's ongoing costs arising out of the Cyber Incident will soon exhaust the limits of the Primary Policy such that C&F's Excess Policy will be implicated.

**The Competing Demands for Payment Under the Policies**

42. FBCS and the Putative Additional Insureds have made several demands for payment of insurance proceeds from the Policies arising out of the Cyber Incident, which claims are for amounts exceeding the \$5 million aggregate limit of the Excess Policy. Specifically, in addition to the costs outlined in Paragraphs 37-41 above, FBCS and the Putative Additional Insureds are seeking insurance coverage for the following matters.

The Underlying Lawsuits

43. To date, 21 lawsuits have been filed against FBCS arising out of the Cyber Incident (the “Underlying Lawsuits”), for which FBCS is seeking defense and indemnity coverage under the Policies. In brief, those lawsuits include:

- a. *Reichbart v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-01876 (E.D. Pa. May 2, 2024) (the “*Reichbart* Action”). The *Reichbart* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5,000,000 exclusive of interest and costs” for FBCS’s alleged failure to secure and safeguard plaintiff’s and approximately 1,955,385 other individuals’ personally identifiable information (“PII”). Exhibit C to this Complaint is a copy of the publicly available complaint in the *Reichbart* Action.
- b. *Stallone v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-01901 (E.D. Pa. May 4, 2024) (the “*Stallone* Action”). The *Stallone* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to properly secure and safeguard plaintiff’s and “nearly 2 million” class members’ PII. Exhibit D to this Complaint is a copy of the publicly available complaint in the *Stallone* Action.
- c. *Croteau v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-01946 (E.D. Pa. May 7, 2024) (the “*Croteau* Action”). The *Croteau* Action is a class action suit brought by plaintiff on behalf of herself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to properly secure and safeguard plaintiff’s and other similarly situated individuals’ personal information from hackers. Exhibit E to this Complaint is a copy of the publicly available complaint in the *Croteau* Action.
- d. *Brooks v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02007 (E.D. Pa. May 10, 2024) (the “*Brooks* Action”). The *Brooks* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” to hold FBCS “responsible for the harms it caused Plaintiff and similarly situated persons in the preventable data breach of Defendant’s inadequately protected computer network.” Exhibit F to this Complaint is a copy of the publicly available complaint in the *Brooks* Action.
- e. *Apthorp v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02024 (E.D. Pa. May 10, 2024) (the “*Apthorp* Action”). The *Apthorp* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] the sum or value of \$5 million, exclusive of interest

and costs” for FBCS’s alleged failure to properly secure and safeguard plaintiff’s and class members’ protected health information (“PHI”) and PII stored within FBCS’s information network. Exhibit G to this Complaint is a copy of the publicly available complaint in the *Apthorp* Action.

- f. *Hwang v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02033 (E.D. Pa. May 13, 2024) (the “*Hwang* Action”). The *Hwang* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million exclusive of interest and costs” for FBCS’s alleged failure to secure and safeguard plaintiff’s PII and the PII of nearly 2.7 million other individuals. Exhibit H to this Complaint is a copy of the publicly available complaint in the *Hwang* Action.
- g. *Vorburger v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02045 (E.D. Pa. May 13, 2024) (the “*Vorburger* Action”). The *Vorburger* Action is a class action suit brought by plaintiff on behalf of herself and all others similarly situated, seeking damages that “exceed[] \$5 million exclusive of interest and costs” for FBCS’s alleged failure to properly secure plaintiff’s and class members’ PII and PHI. Exhibit I to this Complaint is a copy of the publicly available complaint in the *Vorburger* Action.
- h. *Kerr v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02075 (E.D. Pa. May 15, 2024) (the “*Kerr* Action”). The *Kerr* Action is a class action suit brought by plaintiff on behalf of herself and all others similarly situated, seeking damages that “exceed[] the sum or value of \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to prevent the Cyber Incident. Exhibit J to this Complaint is a copy of the publicly available complaint in the *Kerr* Action.
- i. *Vines, et. al v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02085 (E.D. Pa. May 15, 2024) (the “*Vines* Action”). The *Vines* Action is a class action suit brought by plaintiffs on behalf of themselves and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to properly secure and safeguard plaintiffs’ and class members’ PII stored within FBCS’s information network. Exhibit K to this Complaint is a copy of the publicly available complaint in the *Vines* Action.
- j. *Wagner v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02119 (E.D. Pa. May 17, 2024) (the “*Wagner* Action”). The *Wagner* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] the sum or value of \$5 million, exclusive of interest and costs” for FBCS’s allegedly unlawful, willful, and wanton failure to protect the PII of “likely thousands of individuals.” Exhibit L to this Complaint is a copy of the publicly available complaint in the *Wagner* Action.
- k. *Frasier v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02121 (E.D. Pa. May 17, 2024) (the “*Frasier* Action”). The *Frasier* Action is a class action

suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to properly secure and safeguard PII that was entrusted to it. Exhibit M to this Complaint is a copy of the publicly available complaint in the *Frasier* Action.

- l. *Busby v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02129 (E.D. Pa. May 17, 2024) (the “*Busby* Action”). The *Busby* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s allegedly impermissibly inadequate and unlawful data security which caused plaintiff’s and similarly situated individuals’ personal information to be exfiltrated by unauthorized access by cybercriminals. Exhibit N to this Complaint is a copy of the publicly available complaint in the *Busby* Action.
- m. *Courtney v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02153 (E.D. Pa. May 20, 2024) (the “*Courtney* Action”). The *Courtney* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to properly secure and safeguard plaintiff’s and class members’ PII. Exhibit O to this Complaint is a copy of the publicly available complaint in the *Courtney* Action.
- n. *Morgan v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02163 (E.D. Pa. May 21, 2024) (the “*Morgan* Action”). The *Morgan* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” for FBCS’s alleged failure to properly safeguard and secure the PII of approximately 2.7 million individuals. Exhibit P to this Complaint is a copy of the publicly available complaint in the *Morgan* Action.
- o. *Fullwood v. Financial Business and Consumer Solutions, Inc.*, Case No. 2024 CC 002654 CL (Osceola County, Florida County Court, May 29, 2024) (the “*Fullwood* Action”). The *Fullwood* Action is a suit seeking damages between \$8,000 and \$50,000, exclusive of interest, costs, and attorneys’ fees, for FBCS’s alleged failure to secure and safeguard plaintiff’s PII. Exhibit Q to this Complaint is a copy of the publicly available complaint in the *Fullwood* Action.
- p. *Whaley v. Financial Business and Consumer Solutions, Inc.*, Case No. 2024-CC-000662 (Sumter County, Florida County Court, May 29, 2024) (the “*Whaley* Action”). The *Whaley* Action is a suit seeking damages between \$8,000 and \$50,000, exclusive of interest, costs, and attorneys’ fees, for FBCS’s alleged failure to secure and safeguard plaintiff’s PII. Exhibit R to this Complaint is a copy of the publicly available complaint in the *Whaley* Action.

- q. *Soto v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02778 (N.D. Ill. June 6, 2024) (transferred to the E.D. Pa. on June 26, 2024) (the “*Soto* Action”). The *Soto* Action is a class action suit brought by plaintiff on behalf of herself and all others similarly situated, seeking damages that “exceed[] \$5 million, exclusive of interest and costs” as redress for FBCS’s “conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of hundreds of thousands of [FBCS’s] customers.” Exhibit S to this Complaint is a copy of the publicly available complaint in the *Soto* Action.
- r. *Williams v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02642 (E.D. Pa. June 17, 2024) (the “*Williams* Action”). The *Williams* Action is a class action suit brought by plaintiff on behalf of herself and all others similarly situated, seeking damages that “exceed[] the sum of \$5 million exclusive of interest and costs” for FBCS’s alleged failure to properly secure and safeguard plaintiff’s and other similarly situated customers’ PII. Exhibit T to this Complaint is a copy of the publicly available complaint in the *Williams* Action.
- s. *Dozal v. Financial Business and Consumer Solutions, Inc.*, No. 2:24-cv-02775 (E.D. Pa. June 25, 2024) (the “*Dozal* Action”). The *Dozal* Action is a class action suit brought by plaintiff on behalf of himself and all others similarly situated, seeking damages that “exceed[] \$5 million exclusive of interest and costs” for FBCS’s alleged failure to properly secure plaintiff’s and class members’ PHI and PII. Exhibit U to this Complaint is a copy of the publicly available complaint in the *Dozal* Action.
- t. *Hill v. Financial Business and Consumer Solutions, Inc.*, No. CUM-DC-003911-24 (Cumberland County, New Jersey Superior Court, July 22, 2024) (the “*Hill* Action”). The *Hill* Action is a suit by plaintiff seeking \$20,000 in damages arising out of the Cyber Incident. Exhibit V to this Complaint is a copy of the publicly available complaint in the *Hill* Action.
- u. *Cervantes v. Financial Business and Consumer Solutions, Inc.*, Case No. 24CL006255N (San Diego County, California Superior Court, August 9, 2024) (the “*Cervantes* Action”). The *Cervantes* Action is a suit by plaintiff seeking actual damages, statutory damages, costs and attorneys’ fees up to \$74,000 for FBCS’s alleged failure to secure plaintiff’s personal information or provide timely notice of the Cyber Incident. Exhibit W to this Complaint is a copy of the publicly available complaint in the *Cervantes* Action.

44. The damages alleged in the foregoing Underlying Lawsuits total at least \$85,194,000.

45. On July 17, 2024, the U.S. District Court for the Eastern District of Pennsylvania (“E.D. Pa.”) issued an order consolidating the 17 lawsuits outlined above that are venued in the



E.D. Pa., for purposes of pre-trial and discovery purposes only, and appointed Interim Co-Lead Counsel, Executive Committee members, and Liaison Counsel for purposes of, among other things, coordinating communications with and hearings before the court, conducting coordinated discovery, and identifying class members (the “Consolidated Actions”).<sup>2</sup> Exhibit X to this Complaint is a copy of the publicly available foregoing order.

46. On August 16, 2024, plaintiffs in the Consolidated Actions filed a Consolidated Class Action Complaint against FBCS in case number 2:24-cv-01876, alleging FBCS failed to secure and safeguard plaintiffs’ and approximately 4,253,394 other individuals’ PII, then failed to provide adequate and timely notice and details about the Cyber Incident. The Consolidated Class Action Complaint alleges that the aggregate amount in controversy exceeds \$5 million, exclusive of interests and costs, and seeks actual damages, statutory damages, punitive damages, restitution, and disgorgement; equitable, injunctive, and declaratory relief; pre-judgment and post-judgment interest; reasonable attorneys’ fees, costs, and expenses; and such other favorable relief as allowable under law. Exhibit Y to this Complaint is a copy of the publicly available Consolidated Class Action Complaint in the Consolidated Actions.

47. C&F has a reasonable belief that additional lawsuits seeking damages arising out of the Cyber Incident will be filed against FBCS, for which FBCS will seek defense and indemnity coverage under the Excess Policy.

#### The Additional Insured Demands

48. To date, six additional entities have made claims for coverage under the Excess Policy, as purported additional insureds thereunder, seeking payment or reimbursement of costs to

---

<sup>2</sup> The Consolidated Actions include the *Reichbart* Action, *Stallone* Action, *Croteau* Action, *Brooks* Action, *Apthorp* Action, *Hwang* Action, *Vorburger* Action, *Kerr* Action, *Vines* Action, *Wagner* Action, *Frasier* Action, *Busby* Action, *Courtney* Action, *Morgan* Action, *Williams* Action, *Dozal* Action, and *Soto* Action.



notify consumers of the Cyber Incident (the “Additional Insured Demands”). In brief, the Additional Insured Demands are as follows:

- a. On July 29, 2024, counsel for TSI sent C&F an email entitled “Notice of claim under Excess Policy #CYB107007,” seeking, as an additional insured under the Excess Policy, reimbursement or payment of costs to notify consumers of potentially impacted personal data.
- b. On July 29, 2024, counsel for Cascade sent an email to C&F and Travelers, asserting that Cascade is an Additional Insured under the Policies, stating FBCS had advised Cascade it cannot meet its continuing obligations with regard to data breach incident and remediation, and asking whether the Policies had reached their limits or been expended.
- c. On July 30, 2024, Harvest sent a “request for coverage of event expenses” to FBCS’s broker, seeking reimbursement “as a certificate holder” for costs to comply with breach notice laws in relation to individuals potentially affected by the Cyber Incident. The foregoing email was provided to C&F on August 8, 2024.
- d. On August 5, 2024, counsel for Kohl’s sent an email to Travelers and C&F, requesting reimbursement from FBCS’s insurer(s) for its costs to provide credit monitoring, individual notice letters, and similar activities for consumers whose data was potentially impacted by the Cyber Incident.
- e. On August 6, 2024, counsel for Cavalry sent an email to C&F entitled “Remaining Policy Limits/Cavalry Portfolio Services, LLC/FBCS Data Breach,” asserting that Cavalry is an additional insured on FBCS’s cyber insurance and seeking clarity as to whether the Policies have been exhausted in light of outstanding costs to notify potentially impacted individuals.
- f. On August 15, 2024, InvestiNet sent a letter to FBCS, asking that FBCS coordinate, pay for, and handle all consumer notifications and offer credit monitoring for potentially impacted consumers, as required by the contract between InvestiNet and FBCS, and because InvestiNet is named as an additional insured on FBCS’s insurance policies, including its \$10,000,000 in cyber insurance coverage. The foregoing letter was provided to C&F on August 20, 2024.

49. C&F has a reasonable belief that additional entities will similarly seek additional insured coverage under the Excess Policy, or indemnification from FBCS, for their costs of notifying consumers of the Cyber Incident.

The Bankruptcy Case

50. On August 29, 2024, FBCS filed a Voluntary Petition for Chapter 7 bankruptcy in the Bankruptcy Case (“Petition”). Exhibit Z to this Complaint is a copy of the publicly available Petition.

51. According to the public docket for the Bankruptcy Case, Christine C. Shubert has been appointed the trustee of the Chapter 7 estate of FBCS, and, as such, has been named as a defendant in this action given her interest in the limited funds available under the Excess Policy.

**COUNT I – INTERPLEADER**

(28 U.S.C. § 1335)

52. C&F repeats and realleges the allegations contained in paragraphs 1 through 51 of this Complaint for Interpleader as if fully set forth herein.

53. C&F issued an excess liability insurance policy (“Excess Policy”) having a policy limit of \$500 or more.

54. C&F is prepared and will request this Court for leave to deposit the limits of liability of the Excess Policy into the registry account of the Court.

55. There are two or more adverse claimants, of diverse citizenship, who either are demanding, or may demand the insurance proceeds of the Excess Policy.

56. C&F has a legitimate fear that competing demands for payment from the Excess Policy will significantly exceed the limits of liability of the Excess Policy. Thus, any attempt by C&F to make payment in response to one demand from one Defendant may lead to vexatious and multiple litigation actions from other Defendants who also seek to obtain payment from the Excess Policy.

57. C&F stands neutral as to the respective parties who may claim to be entitled to payment under the Excess Policy, and seeks discharge from all obligations under or relating to the Excess Policy.

WHEREFORE, C&F respectfully requests that the Court:

- a. allow C&F to deposit into the registry of the Court the \$5 million aggregate limit of liability of the Excess Policy<sup>3</sup>;
- b. order the Defendants to interplead and adjudge and determine among such Defendants their respective rights to the Excess Policy proceeds and in what amounts;
- c. enter judgment fully and finally discharging C&F and any and all of its current and former agents, representatives or related companies (including, but not limited to, its subsidiaries and parent companies), from all further liability relating in any way to the Excess Policy or any demands that may be made in connection with the Excess Policy;
- d. in accordance with, *inter alia*, 28 U.S.C. § 2361, enter a permanent injunction barring, enjoining, and otherwise restraining Defendants from:
  - i. asserting any claims, rights, causes of action, or demands of whatever nature, whether known or unknown, foreseen or unforeseen, under the Excess Policy against C&F and each of its parents, subsidiaries, affiliates, insurers, reinsurers, directors, officers, employees, agents, representatives, attorneys, and their respective heirs, executors, administrators, successors and assigns; or
  - ii. instituting, commencing, prosecuting any arbitration proceeding, or any legal proceeding in any state or federal court, against C&F and any of its

---

<sup>3</sup> C&F will be separately making a Motion for Leave to Deposit Funds, as required by this Court's Order Regarding Deposit and Investment of Registry Funds.

parents, subsidiaries, affiliates, insurers, reinsurers, directors, officers, employees, agents, representatives, attorneys, heirs, executors, administrators, successors and assigns, with respect to or for any claims, causes of action, rights, attorneys' fees, costs, expenses, judgments, settlements, liabilities and damages, of whatever nature, whether known or unknown, foreseen or unforeseen, that have been, could have been, or could be asserted in any form, either directly or indirectly, based upon, arising out of, relating to, concerning, resulting from or in consequence of, or in connection with:

- (1) the Excess Policy;
- (2) any past, present or future actual or putative notice of **Claim** or notice of circumstances which could give rise to any **Claim** under the Excess Policy;
- (3) any actual or putative **Loss** under the Excess Policy, including, but not limited to defense costs, indemnity or any other payments, services or benefits under the Excess Policy or which otherwise relate to the Excess Policy;
- (4) any alleged right to recover any payments of any defense fees, costs, charges, or expenses made by the Defendants or any future claimants under the Excess Policy;
- (5) any and all duties, liabilities and obligations under the Excess Policy; or
- (6) any and all extra-contractual duties, liabilities, and obligations.

e. award C&F its fees and costs incurred in connection with this interpleader action;  
and

f. grant any and all further relief that this Court may deem equitable and just.

Dated: September 10, 2024

/s/ Brian H. Callaway

TROUTMAN PEPPER HAMILTON SANDERS LLP

Brian H. Callaway (Pa. Bar No. 316034)  
300 Two Logan Square,  
Eighteenth and Arch Streets  
Philadelphia, PA 19103  
(215) 981-4428  
[brian.callaway@troutman.com](mailto:brian.callaway@troutman.com)

Thomas S. Hay (Pa. Bar No. 331456)  
Union Trust Building  
501 Grant Street, Suite 300  
Pittsburgh, PA 15219  
(412) 454-5812  
[thomas.hay@troutman.com](mailto:thomas.hay@troutman.com)

Brandon D. Almond (*pro hac vice* pending)  
401 9th Street, N.W., Suite 1000  
Washington, D.C. 20004-2134  
(202) 274-2864  
[brandon.almond@troutman.com](mailto:brandon.almond@troutman.com)

*Attorneys for Interpleader-Plaintiff Crum & Forster Specialty  
Insurance Company*